SAINTEKS
Volume 15 No 2, Oktober 2018
ISSN: 0852-1468 (159 – 169)

Simulasi Virtual Local Area Network Menggunakan Packet Tracer

(Simulation Virtual Local Area Network Using Packet Tracer)

Harjono[*], Agung Purwo Wicaksono

Program Studi Teknik Informatika, Fakultas Teknik,
Universitas Muhammadiyah Purwokerto,
Jl. Raya Dukuh Waluh Po. Box 202 Purwokerto, Jawa Tengah, 53182

*harjono@ump.ac.id

ABSTRAK

Teknologi jaringan komputer menjadi sebuah kebutuhan utama setiap organisasi. Dengan jaringan komputer, perangkat yang terhubung dapat saling bertukar informasi. Penelitian ini bertujuan untuk mendesain dan menyimulasikan *Virtual Local Area Network* (VLAN) dengan menggunakan Packet Tracer. Dengan menggunakan teknologi VLAN, pengaturan jaringan menjadi sangat fleksibel karena dapat dibuat segmen secara fungsional tanpa bergantung pada lokasinya. Teknologi VLAN dapat meningkatkan keamanan dan kinerja jaringan dengan cara membagi sebuah *broadcast domain* yang besar menjadi beberapa *broadcast domain* yang lebih kecil. *Broadcast domain* yang lebih kecil akan membatasi peralatan yang terlibat dalam aktivitas *broadcast*.

Kata kunci: Packet Tracer, VLAN, broadcast domain

ABSTRACT

Computer network technology becomes a major requirement for every organization. With computer networks, connected devices can exchange information. This study aims to design and simulate Virtual Local Area Networks (VLANs) using Packet Tracer. By using VLAN technology, network settings are very flexible because segments can be functionally created without depending on their location. VLAN technology can improve network security and performance by dividing a large broadcast domain into several smaller broadcast domains. Smaller broadcast domains will limit the equipment involved in broadcast activities

***Keywords**: Cisco, VLAN, broadcast domain*

PENDAHULUAN

Dengan semakin berkembangnya kebutuhan pengolahan data dan informasi, di dalam sebuah perusahaan dibutuhkan banyak komputer yang digunakan oleh banyak orang yang bekerja dalam satu tim. Untuk saling bertukar data dan informasi, maka komputer-komputer yang digunakan akan terhubung antara satu dengan yang lainnya. Kumpulan komputer yang saling terhubung disebut sebagai jaringan komputer (Madcoms, 2010).

Jaringan komputer adalah sistem yang terdiri dari komputer-komputer, serta perangkat yang saling terhubung sebagai satu kesatuan. Dengan dihubungkannya

perangkat- perangkat tersebut maka antar perangkat dapat saling berbagi sumber daya. Jaringan komputer merupakan gabungan antara hardware dan software (Wahana Komputer, 2010).

Penggunaan teknologi VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi atau departemen, tanpa bergantung pada lokasi *workstation*. Teknologi VLAN dapat meningkatkan kinerja jaringan dengan cara membagi sebuah *broadcast domain* yang besar menjadi beberapa *broadcast domain* yang lebih kecil. *Broadcast domain* yang lebih kecil akan membatasi peralatan yang terlibat dalam aktivitas *broadcast*.

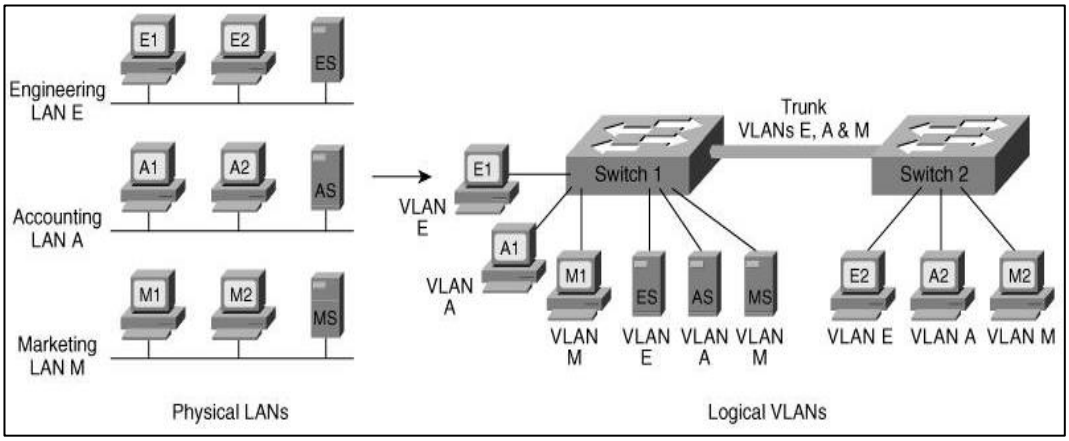
Pada penelitian yang dilakukan Harjono dan Wicaksono (2013) didapatkan sejumlah serangan yang dilakukan oleh *malware* di dalam jaringan lokal. Proses penyebaran *malware* terjadi dengan cara melakukan *broadcast* di dalam jaringan tersebut. Sehingga semua komputer yang berada dalam satu *broadcast domain* yang sama pasti akan menerima paket *broadcast* yang berisi *malware* tersebut. Akibatnya semua komputer dalam jaringan tersebut memiliki kemungkinan yang sangat besar untuk terinfeksi *malware*. Apabila jaringan terbagi ke dalam banyak segmen maka dalam jaringan tersebut memiliki banyak *broadcast domain*, sehingga penyebaran *malware*-pun dapat diminimalisir. Pada penelitian ini dilakukan segmentasi jaringan dengan teknologi Virtual Local Area Network (VLAN).

VLAN dapat diimplementasikan pada *managable switch* dan tidak dapat dibuat pada *non-managable switch*. Karena harga dari sebuah managable switch relativ mahal, maka untuk tujuan pembelajaran lebih dimungkinkan dengan menggunakan software simulasi. Cisco Packet Tracer adalah sebuah software simulasi jaringan multi-tasking yang dapat digunakan untuk menganalisis serta melakukan berbagai macam pekerjaan seperti implementasi topologi yang berbeda, pemilihan jalur optimum berdasarkan algoritma routing, membuat server, subnetting, dan menganalisis konfigurasi jaringan serta perintah-perintah *troubleshooting* (Jain dkk., 2015).

Virtual Local Area Network (VLAN)

Teknologi VLAN (*Virtual Local Area Network*) bekerja dengan cara melakukan pembagian jaringan secara logika ke dalam beberapa *subnet*. VLAN adalah kelompok peralatan dalam sebuah LAN yang dikonfigurasi (menggunakan software manajemen) sehingga mereka dapat saling berkomunikasi seakan-akan dihubungkan dengan jaringan yang sama walaupun secara fisik mereka berada pada segmen LAN yang berbeda seperti pada Gambar 1. Jadi VLAN dibuat bukan berdasarkan koneksi fisikal namun lebih pada koneksi logikaal, yang tentunya lebih fleksibel. Secara logikaa, VLAN membagi jaringan ke dalam beberapa *subnet*. VLAN mengijinkan banyak *subnet* dalam jaringan yang menggunakan *switch* yang sama.

Sebuah VLAN merupakan fungsi logika dari sebuah switch. Fungsi logika ini mampu membagi jaringan LAN ke dalam beberapa jaringan virtual. Implementasi VLAN dalam jaringan memudahkan seorang administrator jaringan dalam membagi secara logika group-group *workstation* secara fungsional dan tidak dibatasi oleh batasan lokasi (Barnes dan Sakandar, 2004).



Gambar 1. VLAN sebagai Implementasi dari Fisikal LAN (Teare dan Paquet, 2005)

METODE PENELITIAN

Dalam penelitian ini menggunakan peralatan berupa sebuah perangkat keras komputer dengan spesifikasi Processor Intel Atom (1,60 GHz), RAM 2 GB, Hardisk 300GB. Sedangkan perangkat lunak yang digunakan adalah perangkat lunak Cisco Packet Tracer versi 7 yang diinstal pada sistem operasi Windows 7.

Penelitian diawali dengan tahapan analisis sistem. Setelah dilakukan subnetting, langkah berikutnya adalah membuat disain topologi jaringan dengan Packet Tracer. Setelah dilakukan konfigurasi pada seluruh perangkat jaringan, langkah terakhir adalah melakukan simulasi.

Analisis dilakukan guna mendapatkan kelemahan, kekurangan atau permasalahan dari jaringan yang ada, khususnya terkait dengan masalah kinerja dan keamanan. Setelah diketahui kekurangannya maka dicari pemecahan atau solusi dari permasalahan tersebut.

Subnetting merupakan sebuah teknik yang digunakan untuk memecah sebuah jaringan menjadi beberapa jaringan yang lebih kecil. Penentuan alamat IP sekaligus juga dilakukan dengan subnetting ini. Setelah proses subnetting selesai dilakukan, langkah berikutnya adalah menentukan VLAN.

Disain atau penggambaran VLAN dilakukan dengan menggunakan *software* Cisco Packet Tracer, yaitu sebuah *software* simulasi jaringan dari Cisco untuk pembelajaran sekaligus *trouble shooting* jaringan. Jadi rancangan jaringan VLAN yang dibuat dengan software tersebut dapat disimulasikan terlebih dahulu sebelum diterapkan di dunia nyata.

HASIL DAN PEMBAHASAN

Analisis Sistem

Sebuah jaringan kampus yang besar namun tidak dibagi menjadi beberapa segmen jaringan (*subnet*) mempunyai kelemahan pada sisi keamanan dan kinerja jaringan. Pada penelitian yang dilakukan Harjono dan Wicaksono (2013) didapatkan sejumlah serangan yang dilakukan oleh *malware* di dalam LAN. Proses penyebaran *malware* terjadi dengan cara melakukan *broadcast* di dalam jaringan tersebut. Sehingga semua komputer yang berada dalam satu *broadcast domain* yang sama pasti akan menerima paket *broadcast* yang berisi *malware* tersebut. Akibatnya semua komputer dalam jaringan terebut memiliki kemungkinan yang sangat besar untuk terinfeksi *malware*. Apabila jaringan terbagi ke dalam segmen-segmen sehingga dalam jaringan tersebut memiliki banyak *broadcast domain*, maka hal tersebut dapat meminimalisir penyebaran *malware*.

Permasalahan keamanan lainnya dapat terjadi ketika seorang yang terhubung ke segmen jaringan maka dia sangat mungkin untuk mengakses seluruh *resource* yang ada pada segmen jaringan tersebut. Contoh kasus, apabila dosen menyimpan file soal ujian pada komputer yang terhubung pada jaringan yang dapat diakses oleh mahasiswa. Berarti antara dosen dan mahasiswa berada pada satu segmen yang sama. Apabila dosen tersebut tidak melakukan pengamanan yang cukup pada file-nya, misalkan karena faktor ketidak tahuan. Maka besar kemungkinan file ujian yang sangat rahasia tersebut dapat diakses oleh mahasiswa. Namun jika dosen dan mahasiswa berada pada segmen jaringan yang berbeda maka kemungkinan untuk terjadi masalah tersebut akan lebih kecil.

Kinerja dari jaringan dapat dipengaruhi oleh jumlah pengguna terlalu banyak untuk setiap segmen jaringan atau *broadcast domain*-nya besar. *Sebuah broadcast* domain yang besar dapat mengganggu jaringan, karena saat sebuah *host* mengirimkan paket ke alamat *broadcast* maka semua *host* yang berada pada alamat *broadcast* yang sama akan mendapat paket tersebut.

Untuk mengatasi permasalahan yang ada maka dapat diatasi dengan membagi jaringan menjadi beberapa segmen jaringan (subnet). Solusi yang digunakan adalah dengan menggunakan teknologi VLAN. Implementasi VLAN dalam jaringan memudahkan administrator jaringan dalam membagi secara logika group-group *workstation* secara fungsional dan tidak dibatasi oleh batasan lokasi fisik. Dalam jaringan kampus ini akan dibagi menjadi empat VLAN yaitu Dosen, Staff, Mahasiswa, dan Tamu, masing-masing dengan vlanId 10, 20,30, dan 40.

Subnetting dan Penentuan VLAN

Subnetting merupakan sebuah teknik yang digunakan untuk memecah sebuah jaringan menjadi beberapa jaringan yang lebih kecil. Penentuan alamat IP sekaligus juga dilakukan dengan *subnetting* ini. *Hasil* alamat *subnet* untuk setiap VLAN yang ada seperti ditunjukkan pada Tabel 1.

Tabel 1 Hasil Penentuan VLAN

Nama VLAN	ID VLAN	Alamat Subnet	Alamat Broadcast
Dosen	10	172.17.10.0/24	172.17.10.255/24
Staff	20	172.17.20.0/24	172.17.20.255/24
Mahasiswa	30	172.17.30.0/24	172.17.30.255/24
Tamu	40	172.17.40.0/24	172.17.40.255/24

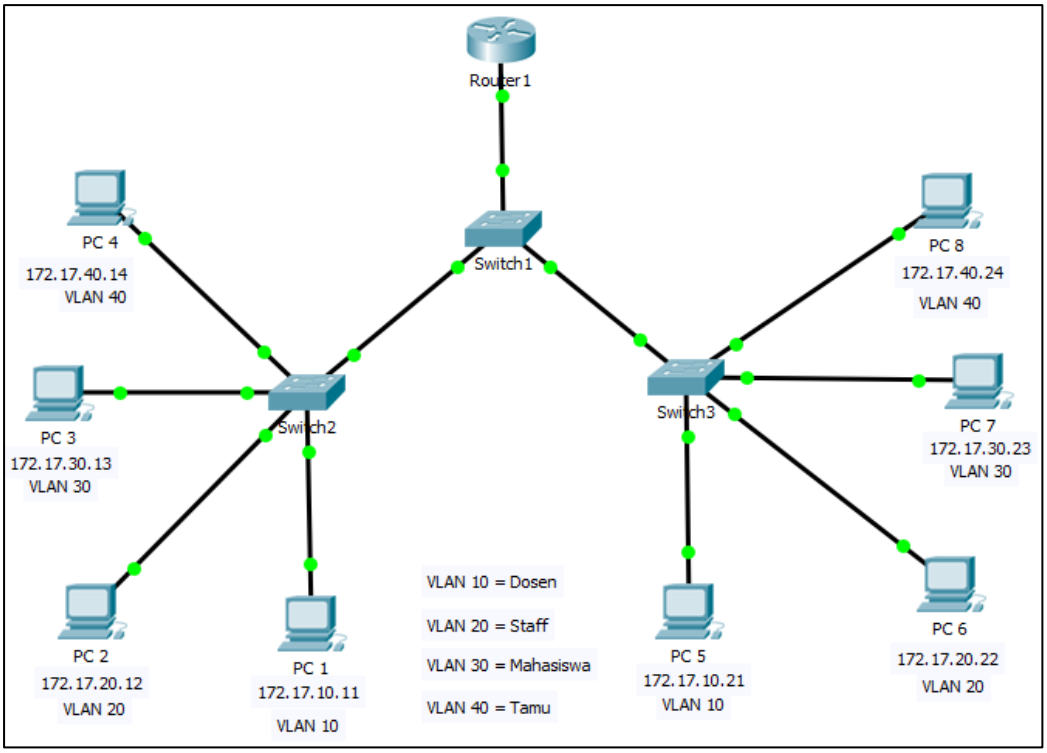
Disain Topologi Jaringan

Penggambaran VLAN dilakukan dengan menggunakan *software* Cisco Packet Tracer, yaitu sebuah *software* simulasi jaringan dari Cisco untuk pembelajaran sekaligus *trouble shooting* jaringan. Hasil gambaran topologi VLAN dapat ditunjukkan pada Gambar 2.

Pada Gambar 2 jaringan dibagi menjadi 4 VLAN yaitu VLAN 10, 20, 30, dan 40. Dengan teknologi VLAN maka sebuah switch dapat terbagi menjadi beberapa jaringan (beberapa *broadcast domain*), dimana hal tersebut tidak dimungkinkan pada LAN konvensional.

Konfigurasi Perangkat

Konfigurasi yang dilakukan pada Switch2 dan Switch3 sama yaitu membuat VLAN, konfigurasi empat port sebagai *access port* dan sebuah port sebagai *trunk port*, dan menugaskan switch port ke VLAN. Sedangkan Switch1 ketiga port dikonfigurasi sebagai trunk port.



Gambar 2. Disain Topologi Diagam VLAN

Perintah untuk membuat VLAN dengan syntax berikut:

Switch# configure terminal
Switch(config)# vlan *[vlan_id]*
Switch(config-vlan)# name *[vlan_name]*
Switch(config-vlan)# end

Setelah itu konfigurasi berikutnya adalah konfigurasi acces port dan trunk port. Konfigurasi access port dengan perintah berikut:

Switch# configure terminal
Switch(config)# interface *[interface_id]*
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan *[vlan_id]*
Switch(config-if)# end

Konfigurasi interface FastEthernet0/24 sebagai trunk port dengan syntax perintah berikut:

Switch# configure terminal
Switch(config)# interface *[interface_id]*
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan *[vlan_id]*
Switch(config-if)# switchport trunk allowed vlan *[vlan-list]*
Switch(config-if)# end

Hasil dari VLAN yang dibuat pada Switch2 seperti diperlihatkan pada Gambar 3, sedangkan hasil verifikasi trunk port seperti pada Gambar 4.

```
Switch2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- ---------
--------------------------------
1    default                          active    Fa0/5, Fa0/6,
Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10,
Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14,
Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18,
Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22,
Fa0/23, Gig0/1
                                                Gig0/2
10   Dosen                            active    Fa0/1
20   Staff                            active    Fa0/2
30   Mahasiswa                        active    Fa0/3
40   Tamu                             active    Fa0/4
88   Management                       active
99   Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Gambar 3. VLAN pada Switch2

```
Switch2#show interface FastEthernet0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Native)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,30,40,88,99
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
 --More--
```

Gambar 4. Verifikasi trunk port

Setelah semua switch selesai dikonfigurasi, langkah selanjutnya adalah melakukan konfigurasi router. Proses ini dinamakan sebagai inter-VLAN routing, yaitu sebuah proses untuk meneruskan lalau-lintas jaringan dari satu VLAN ke VLAN lainnya

menggunakan router. Inter-VLAN routing yang digunakan adalah *router on a stick* dengan ketentuan sebagai berikut:

- Sebuah interface dikonfigurasi sebagai trunk port 802.1Q
- Dibuat subinterface logika, satu subinterface untuk setiap VLAN
- Setiap subinterface dikonfigurasi dengan alamat IP sebagai default gateway bagi masing-masing VLAN
- Interface diaktifkan

Konfigurasi router seperti ditunjukkan pada Gambar 5.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 172.17.10.1 255.255.255.0
Router(config-subif)#interface GigabitEthernet0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 172.17.20.1 255.255.255.0
Router(config-subif)#interface GigabitEthernet0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 172.17.30.1 255.255.255.0
Router(config-subif)#interface GigabitEthernet0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 172.17.40.1 255.255.255.0
Router(config-subif)#interface GigabitEthernet0/0
Router(config-if)#no shutdown
```

Gambar 5. Konfigurasi Router on a stick Inter-VLAN routing

Untuk verifikasi terhadap konfigurasi menggunakan perintah show ip route. Hasil verifikasi seperti pada Gambar 6. Terlihat ada empat route yang terhubung secara langsung dengan router. Dengan teknik router on a stick Inter-VLAN routing ini maka dapat menghemat biaya karena hanya dibutuhkan satu interface router saja untuk menghubungkan banyak VLAN. Sedangkan jika menggunakan legacy inter-VLAN routing maka untuk menghubungkan sejumlah n VLAN dibutuhkan sebanyak n interface router yang tentu saja harganya jauh lebih mahal.

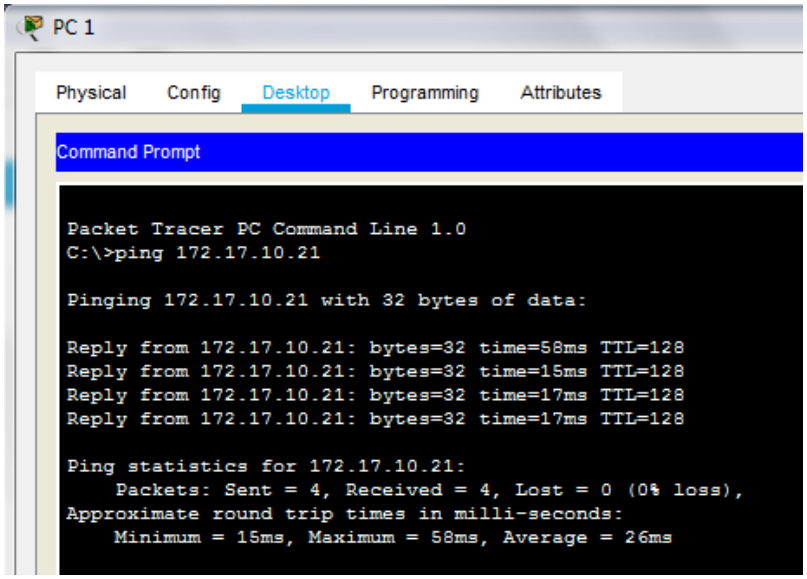
```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.17.0.0/16 is variably subnetted, 8 subnets, 2 masks
C       172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L       172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C       172.17.20.0/24 is directly connected, GigabitEthernet0/0.20
L       172.17.20.1/32 is directly connected, GigabitEthernet0/0.20
C       172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L       172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
C       172.17.40.0/24 is directly connected, GigabitEthernet0/0.40
L       172.17.40.1/32 is directly connected, GigabitEthernet0/0.40

Router#
```

Gambar 6. Tabel Routing

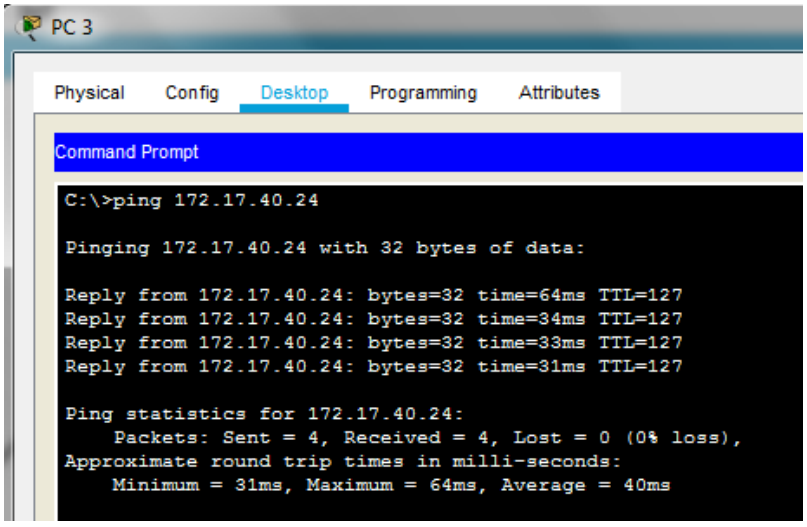
Simulasi VLAN

Simulasi dilakukan dengan melakukan tes konektivitas antar perangkat dalam satu VLAN yang sama dan juga antar perangkat pada VLAN yang berbeda. Tes konektivitas perangkat dalam satu VLAN dengan menggunakan perintah ping dari PC 1 ke PC 5, hasilnya sepertiditunjukkan pada Gambar 7. Sedangkan Tes konektivitas antar perangkat pada VLAN yang berbeda dengan menggunakan perintah ping dari PC 3 ke PC 8, hasilnya sepertiditunjukkan pada Gambar 8.

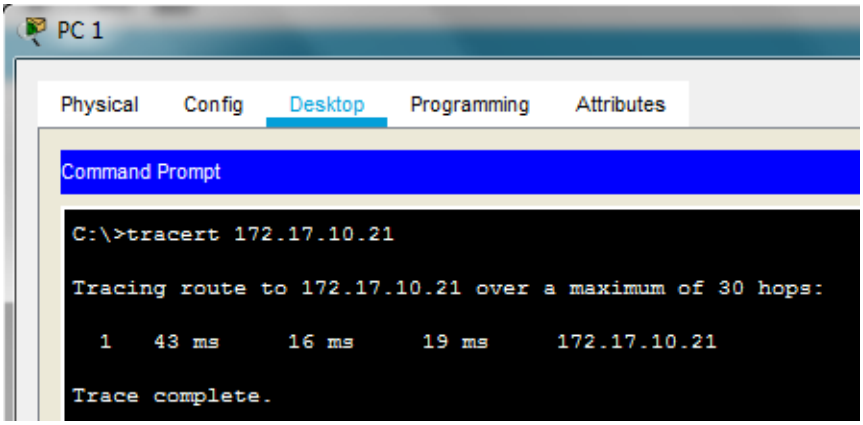
Dengan perintah ping maka perangkat akan mengirimkan ICMP echo request kepada perangkat tujuan. Perangkat yang menerima request tersebut kemudian akan merespon dengan mengirimkan balasan berupa ICMP echo reply. Dari hasil statistik ping antar perangkat yang berada pada VLAN yang sama (VLAN 10) yaitu ping dari PC 1 ke PC 5 *round trip time* rata-rata 26 ms. Sedangkan ping antar perangkat yang berada pada VLAN yang berbeda (VLAN 30 dan VLAN 40) yaitu ping dari PC 3 ke PC 8 *round trip time* rata-rata 40 ms.



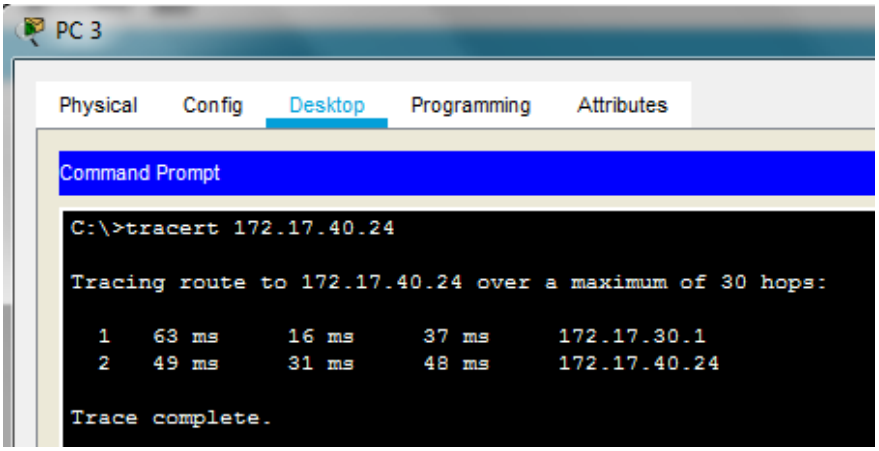
Gambar 7. Hasil ping dari PC 1 ke PC 5



Gambar 8. Hasil ping dari PC 3 ke PC 8

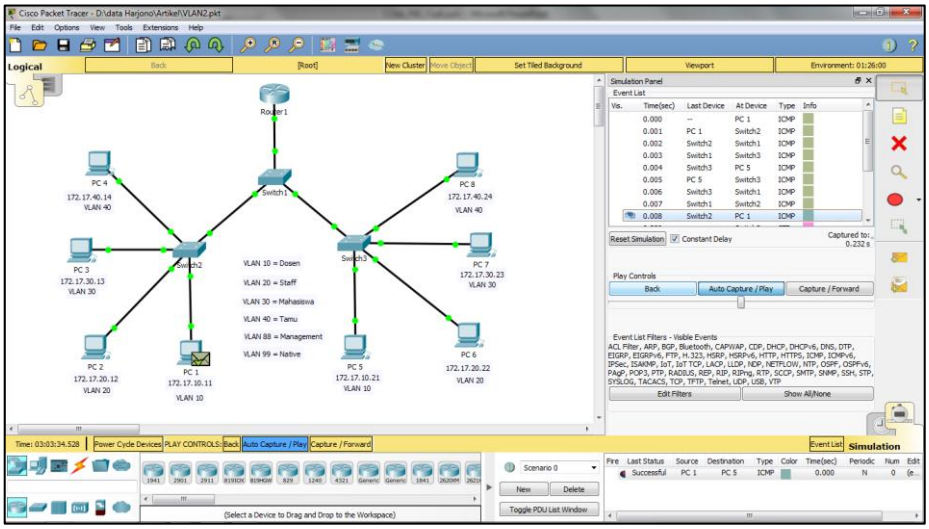


Gambar 9. Hasil tracert dari PC 1 ke PC 5

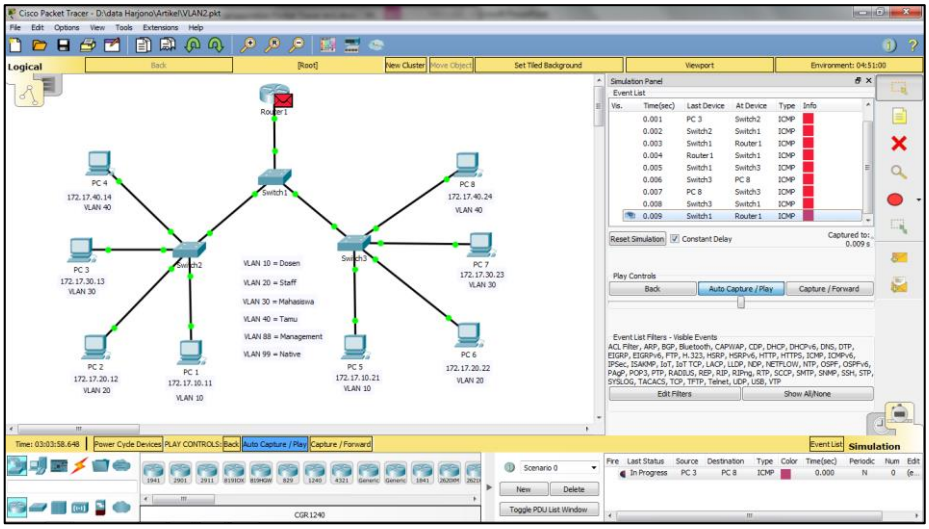


Gambar 10. Hasil tracert dari PC 3 ke PC 8

Round trip time merupakan waktu yang diperlukan oleh perangkat pengirim untuk mengirimkan paket ke tujuan ditambah dengan waktu yang diperlukan oleh perangkat tujuan untuk mengirimkan paket balasan ke pengirim. Terlihat bahwa round trip time untuk ping antar perangkat dalam satu VLAN lebih kecil dibanding dengan round trip time untuk ping antar perangkat dalam VLAN yang berbeda. Hal tersebut terjadi karena komunikasi antar perangkat dalam VLAN yang sama berlangsung tanpa bantuan router seperti ditunjukkan pada Gambar 9 dan Gambar 11. Sedangkan komunikasi antar perangkat dalam VLAN yang berbeda memerlukan bantuan router seperti ditunjukkan pada Gambar 10 dan Gambar 12.



Gambar 11. Simulasi PDU antar perangkat dalam satu VLAN



Gambar 12. Simulasi PDU antar VLAN

KESIMPULAN

Dari hasil penelitian, dapat ditarik kesimpulan sebagai berikut:

a. Dengan menggunakan VLAN, dapat dilakukan segmentasi jaringan berbasis pada fungsional tanpa batasan lokasi secara fisik.
b. Pemecahan jaringan ke beberapa segmen jaringan dapat meningkatkan kinerja jaringan dan keamanan.
c. Untuk menghubungkan antar VLAN dengan router on a stick inter-VLAN routing hanya dibutuhkan satu interface saja.

DAFTAR PUSTAKA

Barnes, D. dan Sakandar, B. 2005. *Cisco LAN Switching Fundamentals*. Cisco Press, USA.

Harjono dan Wicaksono, A.P. 2013. *Honeyd untuk Mendeteksi Serangan di dalam Jaringan Universitas Muhammadiyah Purwokerto*. JUITA Jurnal Informatika ISSN: 2086-9398, Vol II No 4, Nopember 2013.

Jain G, Noorani N., Kiran N., dan Sharma S, 2015, Designing & simulation of topology network using Packet Tracer, *International Research Journal of Engineering and Technology (IRJET)*, ISSN: 2395-0072, Vol 2 No. 2.

Madcoms, 2010, *Sistem Jaringan Komputer untuk Pemula*, Andi Offset, Yogyakarta.

Syafrizal, M. 2005. *Pengantar Jaringan Komputer*. ANDI, Yogyakarta.

Teare D. dan Paquet C. 2005. *Campus Network Design Fundamentals*. Cisco Press.

Wahana Komputer, 2010, *Cara Mudah membangun Jaringan Komputer dan Internet*, Mediakita, Jakarta.